

00862.023286



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Unassigned
Junichi HAYASHI	)	
	:	Group Art Unit: Unassigned
Application No.: 10/686,577	)	
	:	
Filed: October 17, 2003	)	
	:	
For: INFORMATION PROCESSING	)	December 4, 2003
METHOD AND APPARATUS,	:	
COMPUTER PROGRAM, AND	)	
COMPUTER-READABLE	:	
STORAGE MEDIUM	)	

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

Sir:

In support of Applicant's claim for priority under 35 U.S.C. § 119, enclosed is a certified copy of the following Japanese application:

JP 2002-304497, filed October 18, 2002.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicant  
Brian L. Klock  
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200

BLK/lmj

10/686,577

Junichi NAYASHI

INFORMATION PROCESSING METHOD AND APPARATUS,  
COMPUTER PROGRAM, AND COMPUTER-READABLE STORAGE MEDIUM

CFM03286

US

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 1 0 月 1 8 日

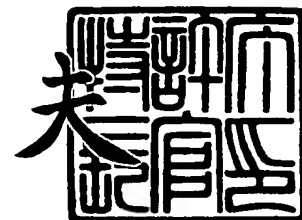
出 願 番 号  
Application Number: 特 願 2 0 0 2 - 3 0 4 4 9 7  
[ST. 10/C]: [ J P 2 0 0 2 - 3 0 4 4 9 7 ]

出 願 人  
Applicant(s): キヤノン株式会社

2 0 0 3 年 1 1 月 4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 9 0 9 7 5

【書類名】 特許願

【整理番号】 4822045

【提出日】 平成14年10月18日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明の名称】 情報処理方法

【請求項の数】 1

【発明者】

【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社  
社内

【氏名】 林 淳一

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100076428

【弁理士】

【氏名又は名称】 大塚 康德

【選任した代理人】

【識別番号】 100112508

【弁理士】

【氏名又は名称】 高柳 司郎

【選任した代理人】

【識別番号】 100115071

【弁理士】

【氏名又は名称】 大塚 康弘

## 【選任した代理人】

【識別番号】 100116894

【弁理士】

【氏名又は名称】 木村 秀二

## 【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0102485

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理方法

【特許請求の範囲】

【請求項1】 タイル単位に圧縮符号化された符号化画像データを入力し、暗号化する情報処理方法であって、

隣接する複数のタイルで1つのタイルグループを構成し、更に、隣接する複数のタイルグループで1つの更なるタイルグループを構成することを繰り返すことでタイル及びタイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義し、

前記符号化画像データで表現される画像全体から、前記ツリー構造の最上位層にあるノードに対する暗号化鍵情報を生成し、

注目ノードの暗号化鍵情報を、上位のノードに対して生成された暗号化鍵情報に基づいて生成することを、末端に位置するノードまで繰り返し行ない、

前記ツリー構造における、前記部分符号化データのノード中の所望とするノード位置を暗号化対象とする指定入力を与えられた場合、当該指定入力されたノード位置の部分符号化データを含み、高位に位置する部分符号化データを暗号化対象として設定し、

暗号化を行うよう設定された個々の部分符号化データに対し、当該部分符号化データに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した部分符号化データ及び暗号化されていない部分符号化データを出力する

ことを特徴とする情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル画像データの圧縮符号化したデータを暗号化する技術に関するものである。

【0002】

**【従来の技術】**

従来、画像データなどを秘匿して伝送するために、画像データ全体の暗号化やスクランブルなどが行なわれてきた。これは、予め画像データ全体を一つの暗号鍵を用いて暗号化し、この暗号鍵に対応する復号鍵を有するものだけが正しく復号することが可能であるようにする技術である。

**【0003】**

しかし、階層構造を有する画像データの場合、その階層構造に応じて画像データの再生の可・不可を制御する目的で、画像全体ではなく階層構造毎に異なる暗号鍵を用いて暗号化処理が行うことが望まれる。また、画像データが複数のタイルから構成され、タイル毎に再生を制御する目的で、タイル毎に異なる暗号鍵を用いて暗号化処理が行われることが望まれる。更に、これらを合わせた場合として、複数のタイルから構成され、更に夫々のタイルが階層構造を有する画像データの場合、タイルと階層構造に応じた画像データの再生を制御する目的で、タイル中の階層構造毎に異なる暗号鍵を用いて暗号化処理が行われる。

**【0004】**

このように、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化することによりタイル、及び階層構造毎に画像データの再生を制御することが可能である。

**【0005】****【発明が解決しようとする課題】**

タイルの符号化データが、複数の部分符号化データで構成される場合において、個々の部分符号化データ毎に異なる暗号鍵を用いて暗号化した場合、暗号化される各部分符号化データの階層構造と、それを復号するための復号鍵との対応付けをする必要があり、その鍵情報の管理が複雑化することは避けられない。

**【0006】**

また、当然のことながら、その鍵情報が正しく管理されていない場合には、正しく復号処理を行うこともできない。

**【0007】**

本発明は上記従来例に鑑みてなされたものであり、個々のタイルが複数の部分符号化データで構成され、その部分符号化データが階層構造を有する画像データ

に対して、各部分符号化データ毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がない技術を提供することを目的とする。

#### 【0008】

##### 【課題を解決するための手段】

この課題を解決するため、例えば本発明の情報処理方法は以下のような工程を備える。すなわち。

#### 【0009】

タイル単位に圧縮符号化された符号化画像データを入力し、暗号化する情報処理方法であって、

隣接する複数のタイルで1つのタイルグループを構成し、更に、隣接する複数のタイルグループで1つの更なるタイルグループを構成することを繰り返すことでタイル及びタイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義し、

前記符号化画像データで表現される画像全体から、前記ツリー構造の最上位層にあるノードに対する暗号化鍵情報を生成し、

注目ノードの暗号化鍵情報を、上位のノードに対して生成された暗号化鍵情報に基づいて生成することを、末端に位置するノードまで繰り返し行ない、

前記ツリー構造における、前記部分符号化データのノード中の所望とするノード位置を暗号化対象とする指定入力を与えられた場合、当該指定入力されたノード位置の部分符号化データを含み、高位に位置する部分符号化データを暗号化対象として設定し、

暗号化を行うよう設定された個々の部分符号化データに対し、当該部分符号化データに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した部分符号化データ及び暗号化されていない部分符号化データを出力することを特徴とする。

#### 【0010】

##### 【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を説明する。

#### 【0 0 1 1】

##### <第 1 の実施形態>

以下、図 1 4 を用いて本実施の形態に適用されるシステム全体について説明する。

#### 【0 0 1 2】

図 1 4 に示すように、本実施の形態におけるシステムは、暗号化処理部（或いは暗号化する装置）1 4 1、アクセス鍵生成部（或いはアクセス鍵生成装置）1 4 2、及び復号処理部（或いは復号装置）1 4 3 から構成される。

#### 【0 0 1 3】

暗号化処理部には、コードストリーム  $c$ （画像データの符号化データであるが、その詳細は後述）が入力され、コードストリーム  $c$  からコンテンツ鍵  $c_k$ 、及び暗号化されたコードストリーム  $c'$  が出力される。アクセス鍵生成処理部 1 4 2 は、このコンテンツ鍵  $c_k$ 、及びアクセスレベル  $a_n$  を入力し、アクセス鍵  $a_k$  を生成する。そして、復号処理部 1 4 3 は、アクセス鍵  $a_k$ 、及び暗号化されたコードストリーム  $c'$  が入力され、復号処理されたコードストリーム  $c''$  が出力される。ここで、 $c' = c''$  である場合、暗号化する以前の画像データに復元されることになる。

#### 【0 0 1 4】

本実施形態においては、アクセス鍵生成部 1 4 2、及び復号処理部 1 4 3 は互いに耐タンパー（耐改ざん）であるようにする。例えば、暗号化処理部 1 4 2 はデジタルカメラで撮影した画像を暗号化し、インターネット上の Web サーバや FTP サーバにアップロードする装置で実行され、アクセス鍵生成処理部 1 4 2 はアクセス鍵を発行するサーバで実行され、復号処理部 1 4 3 は暗号化された画像データをダウンロードするネットワーククライアントで実行されるようにする。

#### 【0 0 1 5】

##### [暗号化処理部]

以下、図 1 を用いて本実施形態に適用される暗号化処理部（機能）を説明する



**【0016】**

図1に示すように、本実施形態における暗号化処理部は、コードストリーム  $c$  を入力し、入力されたコードストリームからコードストリーム鍵  $c_k$ 、及びコードストリーム  $c$  が暗号化された暗号化コードストリーム  $c'$  が生成され、生成されたコードストリーム鍵  $c_k$ 、及び暗号化コードストリーム  $c'$  が出力される。

**【0017】**

本実施形態における暗号化処理部は、暗号化タイルパート指定部 11、鍵行列生成部 12、暗号化部 13 から構成される。

**【0018】**

なお、ここで説明する暗号化処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして捉えたものと考えられるべきものである。

**【0019】**

まずはじめに、暗号化タイルパート指定部 11 の処理の詳細を説明する。暗号化タイルパート指定部 11 には、コードストリーム  $c$  が入力され、入力されたコードストリームから、タイルパートを抽出され、抽出されたタイルパートのうち暗号化対象とするタイルパートを指定するための暗号化タイルパート情報  $t_a$  を出力する。

**【0020】**

そこで先ず、本実施形態におけるコードストリーム、及びタイルパートについて説明する。コードストリームとは、画像データを圧縮符号化した際の符号列である。本実施形態においては、ISO/IEC JTC1/SC29/WG1 10918-1 において標準化されている、通称 JPEG 2000 と呼ばれる圧縮符号化方式によって符号化された符号列のことをコードストリームと呼ぶ。

**【0021】**

JPEG 2000 の圧縮符号化時において、画像は先ず複数の矩形領域に分割され、矩形領域毎にウェーブレット変換により独立に符号化処理が施される。この矩形領域を「タイル」と呼ぶ。更に、符号化されたタイルに対応するコードス

トリームは、少なくとも一つ以上のタイルパートと呼ばれる領域に分割できる。

#### 【0022】

より詳しく説明すると、1つのタイルに対し1回目のウェーブレット変換により得られる成分係数は公知の通り、 $LL1$ 、 $LH1$ 、 $HL1$ 、 $HH1$ の各周波数成分領域を生成する。このうち、 $\{LH1+HL1+HH1\}$ を1つのパートとして扱う。2回めのウェーブレット変換は $LL1$ に対して行うが、このとき生成される $LL2$ 、 $LH2$ 、 $HL2$ 、 $HH2$ のうち $\{LH2+HL2+HH2\}$ も1つのパートとして扱う。

#### 【0023】

また、更に、 $LL2$ に対して更なるウェーブレット変換（3回めのウェーブレット変換）を行う場合には、その結果生じる $\{LH3+HL3+HH3\}$ がパートとして扱われ、残りの $LL3$ が単独のパートとして扱われる。この後、量子化、エントロピー符号化が施され符号化される。上記のタイルパートとは、上記のウェーブレット変換を行う毎に生成された周波数成分の集合の符号化結果を示している。以上が1つのタイルの符号が複数のタイルパートの符号で構成される理由である。

#### 【0024】

なお、JPEG2000では、全タイルに対して固定回数のウェーブレット変換を行うという決まりはない。換言すれば、タイル毎に、ウェーブレット変換の回数は異なってもよいことになっている。

#### 【0025】

以下の実施形態におけるタイルパートとは、上記のような意味を前提にして説明するが、これ以外については後述することとする。

#### 【0026】

タイル、及びタイルパートの具体例を図2を用いて説明する。図2(a)は、ある画像をタイルに分割した際の例である。図2(a)において、21は画像全体を $8 \times 8 = 64$ 個のタイルに分割した例を示している。また、図2(b)は、ある1つのタイルを符号化した際のコードストリームの例を示している。図2(b)に示す例では、1つのタイルは22、23、24、25の4つのタイルパー

トで構成されていることを示している。

#### 【0027】

ここで、タイルパートについて説明する。J P E G 2 0 0 0において、タイルは複数のタイルパートとよばれるいくつかに分割することが可能である。タイルパートは、全てのタイルの中でのタイルパートの順序が保たれさえすれば、異なったタイルからのタイルパートを挟み込むことが可能である。例えば、

タイルインデックス 0 のタイルパートインデックス 0

タイルインデックス 1 のタイルパートインデックス 0

タイルインデックス 0 のタイルパートインデックス 1

タイルインデックス 1 のタイルパートインデックス 1

:

のようにコードストリームを構成することにより、複数のタイルに属するタイルパートを平行に再生することができる。

#### 【0028】

更に、夫々のタイルパートは、ヘッダ部分とデータ部分から構成されている。ここでヘッダ部分とは、データ部分の伸張復号のために必要な種々の情報を格納するための領域であり、タイルパートヘッダと呼ぶ。図 2 (b) では、タイルパート 2 2 が、ヘッダ部分 2 6、データ部分 2 7 で構成されていることを示しているが、他のタイルパートも同様である。

#### 【0029】

また、J P E G 2 0 0 0においては、コードストリーム c はコードストリーム c の復号量に応じて様々な再生方法を実現できるように、所望の再生方法に応じてデータを並べることができる。このようなデータの並べ方をプログレッションオーダと呼ぶ。例えば、復号量の少ない段階では低解像度の画像を再生し、復号量が多くなるにつれてより高解像度の画像を再生するようなプログレッションオーダや、復号量に応じて画質が向上するようなプログレッションオーダでコードストリーム c を構成できる。

#### 【0030】

本実施形態においては、コードストリーム c は、予め、所望のアクセス制御の

方法や度合いに応じたプログレッションオーダ、及びタイルパートで圧縮符号化されていることを前提とする。

#### 【0031】

これに関して、例を用いて説明する。例えば、所定のタイルを3レベルの解像度に応じたアクセス制御をしたい場合を想定する（1つのタイルが3つのタイルパートで構成される場合に相当するものであり、ウェーブレット変換を2回行う場合と考えると分かりやすい）。この場合には、予め、解像度を優先させたプログレッションオーダとなるようにタイルを圧縮符号化し、更にタイルを3つのタイルパートに分割しておく。

#### 【0032】

尚、本実施形態においては入力されるコードストリームcが、予め、所望のアクセス制御の方法や度合いに応じたプログレッションオーダ、及びタイルパートを用いて圧縮符号化されていることを前提としているが、本発明はこれに限定されることはない。即ち、コードストリームcが所望のアクセス制御の方法や度合いに応じたプログレッションオーダやタイルパートを用いて圧縮符号化が施されていない場合には、コードストリームcが入力された後に、所望のアクセス制御の方法や度合いに応じたプログレッションオーダやタイルパートを用いて圧縮符号化し直すようにすれば良い。

#### 【0033】

次にタイルグループについて説明する。本実施形態においては、複数のタイルをグループ化して扱う。グループ化された1つのタイルのグループを「タイルグループ」と呼ぶ。本実施形態においては、グループ化の一例として隣接する2×2の4つのタイルを1つのタイルグループとして扱う。更に、2×2の4つのタイルグループを1つのタイルグループとする。こうして画像全体がひとつのタイルグループとなるまでグループ化を繰り返し行う。

#### 【0034】

タイルグループ化の具体例を図3を用いて説明する。図3の31には、図2に示した例と同様に画像全体を64個のタイルに分割した例を示す。32には、31において隣接する4個のタイルをグループ化し、画像全体を16個のタイルグ

ループで表現した例を示す。更に、33には、32において隣接する4個のタイルグループをグループ化し、画像全体を4個のタイルグループで表現した例を示す。更に、34には、33において隣接する4個のタイルグループをグループ化し、画像全体を1個のタイルグループで表現した例を示す。

#### 【0035】

以上、説明したタイル、タイルパート、及びタイルグループの構成の具体例を図4Aを用いて説明する。

#### 【0036】

図4Aには、画像全体が64個のタイルに分割された場合のタイルグループ、タイル及びタイルパートの構成の例を示す。図4Aに示すように、本実施形態におけるタイルグループ、及びタイルパートは画像全体をルートノードとするツリー構造で表現できる。各ノードがタイルグループ、及びタイルパートに対応する。

#### 【0037】

図4Aにおいてルートノードは画像全体（図3における34）を示す。ルートノード（レベル0）は、レベル1に属する4つの子ノードに対応するタイルグループ（図3における33）から構成されている。ここで、レベルとはツリー構造における各階層構造の段階を示すインデックスである。ルートノードをレベル0であると定義する。更に、ツリー構造における親子の関係を親から子に向かって1回たどる毎に、レベルを1つずつ増やすようにする。

#### 【0038】

すると、レベル1に属するノードは、夫々、レベル2に属する4つの子ノードに対応するタイルグループ（図3における32）から構成されると言い換えることができる。同様に、レベル2に属する4つの子ノードは、夫々、レベル3に属する4つの子ノードに対応するタイル（図3における31）から構成されることになる。そして、レベル4以降は、その直後のレベルに属するひとつの子ノードに対応するタイルパートからだけ構成されている。

#### 【0039】

更に、レベル4以降は、ツリー構造において、大きなタイルパートインデック

スが親ノードに対応し、タイルパートが小さくなる順に、ツリー構造を形成していることに注意する（タイルパートのインデックスが0のタイルパートは、最も低周波成分領域に対応する）。

#### 【0040】

この様に、本実施形態におけるタイルグループ、及びタイルパートはツリー構造で表現できる。

#### 【0041】

更に、タイル、タイルパート、及びタイルグループは夫々を特定することが可能なインデックスが割り当てられる。

#### 【0042】

タイルには、“0”を起源として画像の左上に位置するタイルからラスト順にタイルインデックスが割り当てられる。

#### 【0043】

また、タイルパートには、夫々のタイルにおいて“0”を起源としてコードストリームをデコードする順にタイルパートインデックスが割り当てられる。実施形態では、J P E G 2 0 0 0を例にして説明しているので、タイルパートインデックス“0”は、最も低周波成分領域を指し示すものであり、以下、高周波成分になるにつれてタイルパートインデックスは大きくなる。

#### 【0044】

更に、タイルグループは、夫々を構成する下位レベルのタイルグループ若しくはタイルにおいて“0”を起源として画像の左上に位置するタイル、タイルグループからラスト順にインデックスが割り当てられる。割り当てられたインデックスは、その親のインデックスに連結されて、タイルグループインデックスとして割り当てられる。要するに、復号する際に、必須のもの程、タイルパートインデックスの数字が小さいように割り当てる。

#### 【0045】

以降の説明においては、以上説明したようにタイルグループインデックスが割り当てられるようにするが、本発明はこれに限定されることなく、種々のタイルグループインデックスの割り当て方が可能である。例えば、各ノードの親のタイ

ルグループインデックスに子ノードのグループインデックスを連結させて表現することも可能である。子ノードは、親のタイルグループ内においてラスト順に 0 からインデックスが割り当てられるようにする。

#### 【0046】

この割り当て方によれば、図 4 A における「1-0」で示されるタイルグループは、タイルインデックスで表現すると「0-0」と表現できる。同様に、「2-1」は、「0-0-1」と表現できる。

#### 【0047】

図 4 B は、図 4 A と等価のツリー構造を、タイルインデックス&タイルパートインデックスで示したものである。なお、図示において、例えば「0-0-0-0(3)」における「0-0-0-3」はタイルインデックスであることは上記の通りであるが、末尾の「(3)」はタイルパートインデックスである。タイルパートインデックスが小さいほど優先的に復号する、すなわち、低周波成分の符号化データであることを示している。

#### 【0048】

以上、本実施形態におけるコードストリーム、タイルグループ/タイル/タイルパートの構造、及びタイルグループインデックス/タイルインデックス/タイルパートインデックスについて説明した。

#### 【0049】

本実施形態における暗号化タイルパート指定部 11 では、入力されたコードストリーム c 中のメインヘッダ部分、及びタイルパートヘッダ部分に属する情報を読み出し、タイル、タイルパート、及びタイルグループの構成を解析する。そして、暗号化の対象とするタイルグループ、タイル、及びタイルパートを指定し、暗号化タイルパート情報 t a として出力する。

#### 【0050】

暗号化の対象とするタイルグループ、タイル、及びタイルパートは、ユーザによって明示的に指定されても良いし、RAM や HD などに予め記憶されている情報を用いるようにしても良い。

#### 【0051】

ユーザによって指定されるようにする場合、コードストリーム c を解析した結果を、例えば図 4 B に示すようなツリー構造として、モニタなどを用いてユーザに示すようにする。そして、ユーザは所望のタイルグループ、或いはタイルパートに対応するノードを指定する。或るタイルグループ或いはタイルパートが指定されると、その指定された位置から図示の破線で示される位置に向かう方向に存在するタイルグループ或いはタイルパートも暗号化対象として決定される。

#### 【0052】

例えば、図 4 B において、「0-0-0-0 (2)」が指定された場合、「0-0-0-0 (2)」とその上位にある「0-0-0-0 (3)」が暗号化対象として決定される。ただし、タイル「0-0-0-1 (1)」乃至「0-0-0-3 (0)」は暗号化対象とはならず、解読キーがなくても復号し再現できることを意味する

また、タイルグループ「0-0」が指定された場合には、破線に向かう方向、すなわち、その下位のタイルグループ「0-0-0」、「0-0-1」、「0-0-2」、「0-0-3」が暗号化対象として決定される。ここで、タイルグループ「0-0-0」について着目すると、そのタイルグループにはタイル「0-0-0-0」乃至「0-0-0-3」が含まれるので、それらも暗号化対象として決定され、結果的に、それぞれのタイルの全タイルパートも暗号化対象として決定されることになる。すなわち、1つのタイルグループを指定した場合、そのタイルグループに含まれる下位のタイルグループ、最終的には下位に位置する各タイルの全タイルパートが暗号化対象として決定されることになる。

#### 【0053】

このことは、例えば解像度に応じてアクセス制御をする場合、高解像度に対するアクセス権を有するユーザは、自動的に、低解像度に対するアクセス権を有することを意味する。また、タイルグループを指定した場合には、そのタイルグループに属するタイル、更にタイルパートは全て暗号化対象とすることを意味する。

#### 【0054】

以上、説明した様に暗号化対象となるタイル、或いはタイルパートが決定され



る。暗号化対象として指定されたタイルパートは暗号化対象タイルパート情報  $t_a$  として出力される。ここで、 $t_a$  はタイルインデックスと、そのタイルに属するタイルパートのうち暗号化されるタイルパートのインデックスの最小値との組で構成される。

#### 【0055】

図5に画像全体が64個のタイルから構成されるコードストリームに対する  $t_a$  の一例を示す。図5に示すように、例えばタイルインデックス0のタイルは暗号化されるタイルパートの最小値が0となっており、これはこのタイルに属するタイルパートを全て暗号化することを意味する。一方、タイルインデックス1のタイルは暗号化されるタイルパートの最小値が2となっており、これはこのタイルに属するタイルパートのうちタイルパートインデックスが0、及び1のタイルパートは暗号化されず、タイルパートインデックスが2以上のタイルパートに対して暗号化することを意味する。

#### 【0056】

なお、ユーザが暗号化対象を決定する場合（ $t_a$  を決定する場合）には、特定の暗号化させる1つのタイル、或いは、タイルパートを指定しても良いが、暗号鍵無しで再現できる最高解像度（或いは暗号化鍵で再現する最低解像度）の限界を指定することが望ましい。そこで、図4Bのような画面を表示させたとき、縦一列のタイルグループ或いはタイルパートを一度に設定できるようにするため、縦線を表示し、その表示位置をポインティングデバイスで水平に移動させることで、暗号化する対象を決定するようにすることが望ましいであろう。ただし、ここでは、個々にユーザが指定する場合を説明することとする。

#### 【0057】

以上、説明したように、暗号化タイルパート指定部11から、暗号化対象タイルパート情報  $t_a$  が出力され、暗号化部13に入力される。

#### 【0058】

次に、鍵行列生成部12の処理の詳細を説明する。鍵行列生成部12には、コードストリーム  $c$  が入力され、入力されたコードストリーム  $c$  から、鍵行列  $k_a$  が生成され、生成された鍵行列  $k_a$  及びコードストリーム鍵  $c_k$  が出力される。

## 【0059】

ここで、鍵行列生成部 12 で実行される鍵行列生成処理について図 6 を用いて、詳細に説明をする。図 6 は鍵行列生成部 12 で実行される鍵行列生成処理を示すフローチャートである。

## 【0060】

まず、ステップ S 6 1 でコードストリーム鍵  $c_k$  が生成される。コードストリーム鍵  $c_k$  は、コードストリーム  $c$  のハッシュ値として次式（式（1））の様に算出される。

$$c_k = K(0) = H(c) \quad (\text{式 1})$$

ここで、 $H()$  は、一方向性（不可逆）、及び衝突耐性を有する関数であり、例えば、ハッシュ関数や、DES などの暗号化処理などが適用可能である。コードストリーム鍵  $c_k$  とは、図 4 に示したツリー構造におけるルートノードに対応する値であり、入力した 1 画像分のデータに基づいて生成する。

## 【0061】

次いで、ステップ S 6 2 において、パラメータ  $i$  を初期値 “1”、そしてパラメータ  $j$  を “0” に初期化する。パラメータ  $i$  は前述したツリー構造におけるレベルを示すインデックスであり、パラメータ  $j$  は前述した各レベルにおけるノードを表すインデックスである。特に、 $i$  と  $j$  の組み合わせ  $(i, j)$  をタイルグループインデックスと呼ぶ。

## 【0062】

次のステップ S 6 3 では、タイルグループインデックス  $(i, j)$  のタイルグループ鍵が生成される。タイルグループ鍵は、その親のタイルグループ鍵、及びタイルグループインデックス  $(i, j)$  のハッシュ値として式（2）の様に算出される。

$$K(i, j) = H(K(i-1, k), i, j) \quad (\text{式 2})$$

ここで、 $k$  はタイルグループ  $(i, j)$  の親ノードに対応するノードを表すインデックスである。即ち、親ノードに対応するタイルグループ鍵  $K(i-1, k)$  と、生成するタイルグループ鍵に対応するノードのタイルグループインデックス  $(i, j)$  とからタイルグループ鍵が生成される。しかしながら、本発明はこ

れに限定されることなく、親ノードに対応する鍵と、生成するタイルグループ鍵に対応するノードに含まれるタイルインデックスとからタイルグループ鍵を生成するようにしてもよい。例えば、生成するタイルグループに対応するノードから順に木（ツリー）をたどり、タイルに対応するノードを調べ、当該タイルのタイルインデックスを用いるようにすれば良い。要するに、上位ノード（ルートノード側にあるノード）に対する鍵  $c_k$  と、その下位（下層）方向にあるノードのインデックスに基づいて、下位にあるノードの鍵を派生することを順に繰り返すことになる。

#### 【0063】

ステップ S 6 4 では、レベル  $i$  において全てのノードに対応するタイルグループ鍵が生成されたか否かが判定される。判定結果が真の場合はステップ S 6 6 に進み、判定結果が偽の場合はステップ S 6 5 に進む。

#### 【0064】

ステップ S 6 5 では、パラメータ  $j$  が 1 だけ増やされ、その後ステップ S 6 3 が再度処理される。つまり、パラメータ  $i$  で示されるレベルに属する全タイルグループについて鍵が生成されることになる。

#### 【0065】

一方、パラメータ  $i$  で示されるレベルに対するタイルグループ鍵が生成されると、処理はステップ S 6 6 に進み、変数  $j$  を初期化し、全てのレベルが処理されたか否かが判定される。判定結果が真の場合はステップ S 6 8 に進み、判定結果が偽の場合はステップ S 6 7 に進んで、次のレベルの処理を行うべく、パラメータ  $i$  を 1 だけ増加させ、ステップ S 6 3 以降の処理を繰り返す。

#### 【0066】

さて、処理がステップ S 6 8 に進むとき、末端のノード、すなわち、タイルグループではなく、個々のタイルに対する鍵の生成が行われると、処理はステップ S 6 8 に進む。

#### 【0067】

ステップ S 6 8 では、パラメータ  $m$  を “0”、パラメータ  $n$  を “ $N-1$ ” で初期化する。ここで、パラメータ  $N$  とは、タイル  $m$  を構成するタイル部分の総数

である。

#### 【0068】

ステップS69では、タイルインデックス $m$ 、タイルパートインデックス $n$ に相当するタイルパート鍵が生成される。タイルパート鍵は、その親のタイルパート鍵のハッシュ値として式(3)の様に算出される。

$$K(m, n+1) = H(K(m, n)) \quad (\text{式3})$$

生成されたタイルパート鍵は鍵行列 $k_a$ として記録される。ここで、鍵行列 $k_a$ の例を図7を用いて説明する。図7には本実施形態に適用可能な鍵行列 $k_a$ の一例を示す。従って、或るタイルパートの最も大きなインデックスを持つタイルパートの鍵は、そのタイルパートが属するタイルに対して生成された鍵(ステップS63で生成された鍵)を元に生成し、以下、タイルパートのインデックスが小さくものは、それより1つ大きなインデックスのタイルパートに与えられたキーを用いて派生することになる。

#### 【0069】

図7は、画像全体が64個のタイルから構成され、タイルパートの数の最大が5である場合の鍵行列 $k_a$ の例を示している。図7に示すように、鍵行列 $k_a$ の各行はタイルに相当し、各列はタイルパートに相当する。行列の要素値としては、ステップS68で算出したタイルパートの鍵を記録する。タイルパートが存在しない要素にはNULLなど記録するようにする。

#### 【0070】

ステップS69に続いてステップS70が処理される。このステップS70では、タイルパートインデックス $n$ に属する全てのノードに対応するタイルパート鍵が生成されたか否かが判定される。判定結果が真の場合はステップS72に進み、判定結果が偽の場合はステップS71に進んでパラメータ $n$ を“1”だけ減じ、ステップS69の処理を行うことになる。

#### 【0071】

こうして、タイルインデックス $m$ で示される全タイルパートに対する処理が終わると、ステップS72に進み、変数 $n$ を初期化し、全てのタイルが処理されたか否かが判定される。判定結果が真の場合は、鍵行列生成処理を終了し、判定結

果が偽の場合はステップ S 7 3 に進み、次のタイルに対する処理を行うべくパラメータ  $m$  を “1” だけ増加させ、ステップ S 6 9 以降の処理を繰り返すことになる。

#### 【0072】

以上、説明したように、鍵行列生成処理により鍵行列  $k_a$  が生成される。生成された鍵行列  $k_a$  は暗号化部 1 3 に入力される。

#### 【0073】

次に、暗号化部 1 3 の処理の詳細を説明する。暗号化部 1 3 は、コードストリーム  $c$ 、暗号化対象タイルパート情報  $t_a$ 、及び鍵行列  $k_a$  を入力し、暗号化タイルパート情報  $t_a$  に示されたコードストリーム  $c$  のタイルパートを、鍵行列  $k_a$  に記録されているタイルパート鍵を用いて暗号化し、暗号化されたコードストリーム  $c'$  を出力する。具体的には次の通りである。

#### 【0074】

暗号化部 1 3 は、まず、暗号化タイルパート指定部 1 1 からの暗号化タイルパート情報  $t_a$  に基づき、実際に暗号化対象となるタイルパートであるかどうかを判断するための暗号化タイルパート行列を生成する。暗号化タイルパート行列の例は図 8 に示す通りである。図示の行列において、行はタイルを表し、列はタイルパートを表す。更に、要素の値としては、暗号化対象とならないタイルパートは 0、暗号化対象となるタイルパートは 1、存在しないタイルパートは 2 で示されている。「2」が格納される理由は、タイルをウェーブレット変換する際の変換回数がタイル毎に異なる、すなわち、各タイルのタイルパートの個数が異なっても構わないことに対処するためである。因に、図 8 の場合には、ウェーブレット変換の最大回数は 5 回であることを示している（ウェーブレット変換回数 + 1 がタイルパートの個数であることは既に説明した）。

#### 【0075】

暗号化タイルパート情報  $t_a$  には、各タイル中で暗号化されるタイルパートインデックスの最小値が記録されており、更に本実施形態においては、夫々のタイル中で、暗号化タイルパート情報  $t_a$  に記録されたタイルパートインデックスよりも大きな値を持つタイルパートは暗号化されるために、図 5 に示す暗号化タイ

ルパート情報からは、図 8 に示すように暗号化対象となるタイルパートが特定される。

#### 【0076】

次に、暗号化対象タイルパート行列と鍵行列  $k_a$  を比較し、暗号化対象タイルパート行列の要素値が 1 であるタイルパートに対して、鍵行列  $k_a$  中の同じ座標に位置する鍵を用いて、コードストリーム  $c$  中のタイルパートを暗号化する（暗号化対象タイルパート行列の要素値が 0 のタイルパートについては暗号化しない）。こうして、暗号化対象となっているタイルパート全てに対して暗号化を施し、コードストリーム  $c$  中の該当するタイルパートのデータは、暗号化されたタイルパートのデータで置換えられ、出力される。

#### 【0077】

また、暗号化したタイルパートは、該タイルパートが暗号化されていることを示すための情報  $I_n f$  をタイルパートヘッダに記録しておく。これは、後述する暗号復号処理の際に、タイルパートが暗号化されているか否かを判定するために用いる。

#### 【0078】

更に、J P E G 2 0 0 0 においては、タイルパートを構成するコードストリーム  $c$  は、パケットと呼ばれる単位から構成されている。そして、パケットはヘッダ部分とデータ部分から構成されている。本実施形態においては、ヘッダ部分は暗号化せずに、データ部分だけを暗号化するようにする。このように暗号化することによって、例え暗号化したとしても、画像として正しく伸張復号することが可能である。

#### 【0079】

暗号化の方法としては、本実施形態においては特に限定せず、D E S (D a t a E n c r y p t i o n S t a n d a r d) や、A E S (A d v a n c e d E n c r y p t i o n S t a n d a r d) など種々の暗号アルゴリズムを適用可能である。

#### 【0080】

以上の様に、暗号化タイルパート行列に示された全てのタイルパートが暗号化

されたコードストリームは、暗号化コードストリーム  $c'$  として出力される。以上、図 14 における暗号化処理部 141 について説明した。

#### 【0081】

上記本実施形態における暗号化処理部 141 は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納する CDROM 等のコンピュータ可読記憶媒体にまで及ぶものである。

#### 【0082】

##### [アクセス鍵生成処理部]

次に、図 9 を用いて本実施形態に適用されるアクセス鍵生成部（機能）を説明する。

#### 【0083】

図 9 に示すように、アクセス鍵生成部は、コードストリーム鍵  $c_k$ 、及びアクセスを許可するインデックス  $a_n$  が入力され、入力されたコードストリーム鍵  $c_k$  からアクセスを許可するインデックス  $a_n$  に対応するアクセス鍵  $a_k$ （暗号化を解除する鍵）が生成され、生成されたアクセス鍵  $a_k$  が出力される。ここで、アクセスを許可するインデックス  $a_n$  とは、アクセスを許可するタイルグループインデックス、或いはタイルとタイルパートインデックスである。

#### 【0084】

図 4 に示したように、本実施形態においては、タイルグループ、及びタイルパートはツリー構造で表現できる。図 4 に示したツリー構造を構成するノードのうち、ひとつのノードを、アクセスを許可するインデックス  $a_n$  で指定し、指定されたノードに対応するアクセス鍵を生成する。

#### 【0085】

指定されたノードのアクセス鍵を生成する方式としては、入力されたコードストリーム鍵  $c_k$  をルートノードに対応させ、図 6 に示したような方法で順に各ノードに対応する鍵を生成し、これをノードのインデックスがアクセスを許可する

インデックス  $a_n$  になるまで繰り返すようにすれば良い。

#### 【0086】

生成されたアクセス鍵は、図10に示すようなフォーマットに従って  $a_k$  として出力される。図10に示すように、 $a_k$  は、アクセス鍵、アクセス鍵が対応するタイルグループ或いはタイルパートのインデックス、及びタイルパートインデックスかタイルグループインデックスかを示す情報から構成される。図10に示すようなフォーマットに格納された後、 $a_k$  は後述する暗号復号処理部に渡される（実際は、暗号復号処理部からの要求に応じて提供する）。出力されたアクセス鍵は安全に暗号復号処理部に送信するために、暗号化されて  $a_k$  に記録するようにしても良い。

#### 【0087】

アクセス鍵生成部におけるアクセス鍵生成処理について、例を用いて説明する。

#### 【0088】

例えば、アクセスを許可するインデックス  $a_n$  として、タイルグループインデックス「0-0-0」（図4B参照）を指定したとする。すると、入力されたコードストリーム鍵  $c_k$ （ルートノードに対応する）から、タイルグループインデックス「0-0」に対応するタイルグループ鍵をハッシュ関数を用いて生成する。更に、生成されたタイルグループ「0-0」のタイルグループ鍵から、タイルグループ0-0-0のタイルグループ鍵を生成し、それをタイルグループ鍵0-0-0のアクセス鍵  $a_k$ （図10）として出力する。

#### 【0089】

##### [暗号復号処理部]

まず、実施形態における暗号復号処理部143と、アクセス鍵生成処理部142との大まかな動作を説明し、その後で、具体的な暗号復号処理部143の処理内容を説明することとする。暗号復号処理部143はインターネットに接続し得る一般のユーザが所有しているPC、アクセス鍵生成処理部142は暗号化を解除するための認証サーバとして考えると分かりやすいので、それを前提にして説明する。



## 【0090】

暗号化されたコードストリーム  $c'$  を受信した暗号復号処理部（クライアント PC）143は、非暗号化のタイルパートの符号データに基づいて画像を再現する。従って、再現できる画像の解像度は自ずと限られていることになる。このとき、その暗号復号処理部のユーザが、より高い解像度を再現できるよう望む場合、暗号化されているタイルパートから上位に遡って、要求するレベルのノードをユーザからの指示に従い決定する。このノードのレベル（タイルグループインデックスかタイルパートインデックス）をアクセス鍵生成処理部142（認証サーバ）にインデックス  $a_n$  として要求する。この結果、アクセス鍵生成処理部142からは、要求したノードに対するアクセス鍵  $a_k$  が送られてくるので、受信したアクセス鍵  $a_k$  に基づき、その下位に向かう暗号を解除するための鍵群を生成する。そして、その鍵を用いて符号データの暗号化を解除し、復号を行なう。

## 【0091】

なお、アクセス鍵生成処理部142としては、アクセス鍵  $a_k$  を取得したい旨の要求をクライアント（復号処理部に対応する）から受信した場合、認証処理や課金等の処理を経て、そのアクセス鍵を提供することになるであろう。従って、このアクセス鍵生成処理部142をインターネットに認証サーバとして設置する場合、複数の暗号化処理部、複数の復号処理部を想定して設置する必要がある、必然、多数の画像を特定する情報と共に、それら個々の画像に対するコードストリーム鍵を登録できるようにしておく。そして、復号処理部143は、画像を特定する情報と暗号を解除するためのノードインデックスを通知することで、目的とする画像の目的とするノードレベルのアクセス鍵  $a_k$  を得るようになる。アクセス鍵生成処理部142（認証サーバ）としては、1つの画像について、その画像を特定する情報（IDやファイル名等）と、その画像のルートノードに対する1つのコードストリームだけ記憶していれば良いので、記憶管理する情報量も少なくできよう。

## 【0092】

上記を踏まえ、以下、図11を用いて本実施形態に適用される暗号復号処理部（機能）を説明する。

**【0093】**

図11に示すように、本実施形態における暗号復号処理部は、鍵行列生成部111、暗号復号部112、及び暗号化タイルパート判定部113から構成される。

**【0094】**

まずはじめに、鍵行列生成部111の処理の詳細を説明する。鍵行列生成部111には、アクセス鍵生成処理部142に要求したタイルグループインデックス、或いはタイルパートインデックスに対するアクセス鍵 $a_k$ が入力される。そして、入力されたアクセス鍵 $a_k$ から、鍵行列 $k_{a'}$ （各ノード（タイル及びタイルパート）に対応する解読キー）を生成し、その生成された鍵行列 $k_{a'}$ を出力する。

**【0095】**

ここで、鍵行列生成部111で実行される鍵行列生成処理について図12を用いて、詳細に説明をする。図12は鍵行列生成部111で実行される鍵行列生成処理を示すフローチャートである。

**【0096】**

まず、ステップS121で入力されたアクセス鍵 $a_k$ がタイルグループに対応するものか、或いはタイルパートに対応するものかが判定される。この判定のためには、図10に示した「タイルパートインデックスかタイルグループインデックスかを示す情報」を利用する。判定結果がタイルグループインデックスの場合にはステップS122に進み、判定結果がタイルパートインデックスの場合にはステップS128に進む。

**【0097】**

ステップS122（タイルグループインデックスの場合）では、パラメータ $i$ 、及びパラメータ $j$ を、図10に示したアクセス鍵フォーマット中の「アクセス鍵値に対応するインデックス」に初期化する。パラメータ $i$ は前述したツリー構造におけるレベルを示すインデックスであり、パラメータ $j$ は前述した各レベルにおけるノードを表すインデックスである。即ち、 $i$ と $j$ の組み合わせ（ $i, j$ ）はタイルグループインデックスである。

## 【0098】

一方、タイルパートインデックスであると判断し、ステップS128に進んだ場合には、パラメータm、及びパラメータnを、図10に示したアクセス鍵フォーマット中の「アクセス鍵値に対応するインデックス」に初期化にする。ここで、パラメータmはタイルインデックス、パラメータnはタイルグループインデックスを示す。

## 【0099】

その他の処理は、図6における鍵生成処理と同様の処理であるので詳細な説明は省略する。

## 【0100】

以上、説明したように、鍵行列生成処理により鍵行列k a'が生成される。生成された鍵行列k a'は暗号復号部112に入力される。

## 【0101】

次に、暗号化タイルパート判定部113の処理の詳細を説明する。暗号化タイルパート判定部113には、暗号化されたコードストリームc'が入力され、入力されたコードストリームc'からタイルパートが抽出され、抽出されたタイルパートが暗号化されているか否かが判定され、暗号化タイルパート情報t a'が出力される。

## 【0102】

本実施形態における暗号化部分判定部113では、入力されたコードストリームc'中のタイルパートヘッダ部分を解析し、タイルパート部分に「タイルパートが暗号化されていることを示す情報」Infが記録されているか否かを調べる。判定された情報は、暗号化タイルパート情報t a'として出力される。暗号化タイルパート情報t a'の一例を図13に示す。

## 【0103】

図13は、画像全体が64個のタイルから構成され、タイルパートの数の最大が5である場合の暗号化タイルパート情報t a'の例を示す。図13に示すように、暗号化タイルパート情報t a'の各行はタイルに相当し、各列はタイルパートに相当する。行列の要素値としては、暗号化されていない場合には0を、暗号

化されている場合には1を、存在しないタイルパートには2を記録する。

#### 【0104】

次に、暗号復号部112の処理の詳細を説明する。暗号復号部112には、暗号化されたコードストリーム $c'$ 、鍵行列 $k_a'$ 、及び暗号化タイルパート情報 $t_a'$ が入力され、暗号化タイルパート情報 $t_a'$ に示されたコードストリーム $c'$ のタイルパートが、鍵行列 $k_a'$ に記録されているタイルパート鍵を用いて復号され、復号されたコードストリーム $c'$ が出力される。

#### 【0105】

暗号化処理部13では、暗号化タイルパート行列 $t_a'$ と鍵行列 $k_a'$ を比較し、暗号化タイルパート行列 $t_a'$ の要素値が1であるタイルパートに対して、鍵行列 $k_a'$ 中の同じ座標に位置する鍵を用いて、コードストリーム $c$ 中のタイルパートを暗号復号処理する。そして、コードストリーム $c'$ のタイルパートは、暗号復号処理されたタイルパートに置き換えられる。

#### 【0106】

また、暗号復号処理したタイルパートは、タイルパートヘッダに記録されている、該タイルパートが暗号化されていることを示す為の情報 $I_n f$ を消去する。

#### 【0107】

更に、ヘッダ部分は暗号復号処理せずにデータ部分だけを暗号復号処理するようにする。

#### 【0108】

暗号復号処理の方法としては、暗号化処理部で実行した方法に対応する方法でなければならない。

#### 【0109】

以上の様に、アクセス鍵に応じて、暗号化されたコードストリーム $c'$ が暗号復号され、暗号復号されたコードストリームは、暗号復号コードストリーム $c''$ として出力される。

#### 【0110】

従って、図14における復号処理部143が、アクセス鍵生成処理部142からアクセス鍵 $a_k$ を受信しないで、暗号化されたコードストリーム $c'$ を受信し

復号処理したとしても、暗号化されていないタイルパートについては復号が成功するだけとなり、予め許容された解像度以下の画像の再現までが可能となる。換言すれば、復号処理部 143 のユーザが、より鮮明な画像を望む場合には、アクセス鍵 a k を取得し、再度復号化処理を行えば良いことになる。

#### 【0111】

以上説明したように本第 1 の実施形態によれば、複数のタイル及び階層構造を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がないようにすることが可能となる。更に、複数のタイル及び階層構造と、それらに対応する復号鍵を記録し、正しく復号処理を実行することか可能となる。

#### 【0112】

なお、上記の実施形態でのタイルパートとは、ウェーブレット変換処理を行った際に生成される各周波数成分領域の集合単位とするものであったが、これに限定されるものではない。

#### 【0113】

例えば、一般に画像の圧縮符号化では、ウェーブレット変換や直交変換等の周波数変換処理して得られたデータを量子化し、エントロピー符号化を施すが、量子化して得られた各係数値のビット単位のプレーン毎に符号化することを行う提案も既に幾つかなされており、これに適用させても良いからである。より具体的に説明するため、図 15 を用いて説明する。

#### 【0114】

図 15 は、量子化した後の係数値のブロックを示している。図示では説明を単純化するため、 $4 \times 4$  としているが勿論、これより大きくても構わないし、一般に、このサイズよりも大きなものとなる。座標  $(i, j)$  として表現したとき、図示は、 $(1, 1)$  の係数値が「5」、 $(3, 1)$  が「3」、 $(1, 3)$  が「2」という値を持ち、それ以外は「0」となっている例を示している。この中で値が最も大きいものが「5」であり、バイナリー（2進）で表記すると「101」となる。つまり、図示の場合、全ての係数が 3 ビットで表現できるので、ビット 2 のプレーン、ビット 1 のプレーン、ビット 0 のプレーンの 3 つのプレーンがあ

れば十分に表現でき、ビットプレーン毎に符号化を行う。

#### 【0115】

一方、データの重要度から見た場合、高位のビットほどその重要であるから、結局のところ、ビット2のプレーンがそのブロックの画質に支配的となり、以下、画質に与える影響の大きな順は、ビット1のプレーン、ビット0のプレーンとなる。これは、ちょうど、先に説明したウェーブレット変換を複数回行った際の、最も低周波成分の係数値（LL成分）が、ビット2のプレーンであり、最も高周波成分の係数の集合  $\{LH1 + HL1 + HH1\}$  がビット0のプレーンに対応するのと同様の意味を持つことに他ならない。

#### 【0116】

一方、周波数変換し、量子化した後の値の最大値によって、符号化する対象のプレーンの数が決定されるわけであるから、そのプレーンの数は個々のタイルによって異なる。仮に、固定の量子化ステップで量子化し、その時に取り得る値が0乃至63であるとしたとき、最大で6つのプレーン（ビット0～5のプレーン）が発生し得ることになる。図15は、このような状況において、たまたま全ての係数が3ビット（ビット0乃至2）以内で表現でき、ビット3乃至5のプレーンは生成する必要はない。すなわち、使用していないビットプレーンについては、そのデータが存在しなくても良いから、先に説明した図8に示した暗号化タイルパート行列内に「2」が格納される。

#### 【0117】

従って、タイルパートは、上記のように、符号化する際に用いたビットプレーンの数を割り当て、最も上位のビットプレーンに対して小さなタイルパートのインデックスを割り当てることでも、全く同様の効果が期待できる。或いは、符号化する際に用いたビットプレーンのいくつかのまとまりをレイヤとし、最も上位のレイヤに対して小さなタイルパートのインデックスを割り当てるようにしてもよい。

#### 【0118】

また、画像を符号化する際、原画像中の $M \times N$ 画素で表現される部分画像（プレシント）を更に幾つかに分割し、個々の分割領域をタイルパートとして定義

しても構わない。

### 【0119】

さらに、複数の成分（輝度成分や、色成分など）から構成される画像を符号化  
する際、所定の成分（例えば、輝度値）をタイルパートとして定義しても構わな  
い。

### 【0120】

以上を簡単にまとめると、実施形態における暗号化対象の指定とその暗号化処  
理は2通り存在することになる。

### 【0121】

1つ目は、或るタイルグループを暗号化対象として指定したとき、そのタイル  
グループに属する下位のレベルのタイルグループ、最終的には指定されたタイル  
グループに属する全タイルが暗号化対象として設定される。そして、ルート（レ  
ベル0）のタイルグループに対して生成された暗号化キーから派生して生成され  
たキーを用いて、暗号化対象のタイルデータが暗号化される。

### 【0122】

この結果、暗号化キーとしては1つで済み、尚且つ、所望とするタイルグルー  
プに属するタイルについて暗号化させることができる。

### 【0123】

2つ目は、或るタイルパートに対して暗号化対象として指定したとき、その指  
定されたタイルパートのインデックス以上のインデックスを有するタイルパート  
を暗号化させることができることである。換言すれば、暗号化対象として指定し  
たタイルパートより小さいインデックスを有するタイルパートについては非暗号  
化となるので、解像度の低い画像については無条件に再現できるものの、それを  
越える解像度について、解読キーを有しない限り不可にできる。

### 【0124】

#### [第2の実施形態]

第1の実施形態においては、図1において鍵行列指定部12と暗号化部13を  
分離させ、鍵行列指定部12の出力である鍵行列kaを暗号化部13に入力する  
ようにしていた。また、図11における鍵行列ka'も同様である。鍵行列ka

、及び鍵行列  $k a'$  の大きさは画像を構成するタイル数とタイルパートの最大値によって決定する。よって、多くのタイルを有する画像であったり、タイルパートの最大値が場合には、鍵行列  $k a$ 、及び鍵行列  $k a'$  の大きさが大きくなってしまふことがある。

#### 【0125】

しかしながら本発明は、これに限定されることなく、鍵行列生成部 12、及び鍵行列生成部 111 は必ずしも鍵行列  $k a$ 、及び鍵行列  $a'$  を全画像分まとめて出力する必要はない。ひとつの鍵が生成される度に、生成された鍵を暗号化部 13、或いは暗号復号部 112 に出力するようにすることも可能である。このようにすることによって、鍵のために必要とされるメモリ量を小さくすることが可能となる。

#### 【0126】

以上説明したように本実施形態によれば、複数のタイル及び階層構造を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要があるようにすることが可能となる。更に、複数のタイル及び階層構造と、それらに対応する復号鍵を記録し、正しく復号処理を実行することか可能となる。

#### 【0127】

##### [第3の実施形態]

第1の実施形態においては、タイルグループ鍵、及びタイル鍵の生成のために(式2)を用い、タイルパート鍵の生成のために(式3)を用いるようにした。

#### 【0128】

しかしながら、本発明はこれに限定されることはなく、鍵生成のために種々の処理を行うことが可能である。例えば、図6におけるS63において、タイル鍵を、その親のタイル鍵のハッシュ値として(式2')の様に算出しても良い。

$$K(j+1) = H(K(j)) \quad (\text{式2'})$$

ここで、 $j$  はタイルインデックスである。また、図6におけるS69において、タイルパート鍵を、タイル鍵とタイルパートインデックスのハッシュ値として(式3')の様に算出しても良い。



$$K(m, n) = H(K(m), n) \quad (\text{式 } 3')$$

ここで、 $m$ はタイルインデックス、 $n$ はタイルパートインデックスである。

#### 【0129】

このように生成された鍵のツリー構造を図16に示す。図16は、4つのタイルと、夫々のタイルが3つのタイルパートから構成されるコードストリーム $c$ に対応する鍵を、前記(式2')及び(式3')を用いて生成した際の鍵のツリー構造を示す図である。

#### 【0130】

以上のような処理とすることにより、各々タイルに対する鍵は親のノードに対応するタイル鍵からハッシュ関数だけによって生成することができる。例えば、タイルインデックス2とタイルインデックス3に対応するタイルへのアクセスを許可するような場合に、第1の実施形態においては、アクセス鍵生成処理部において、タイルインデックス2とタイルインデックス3に対応する2つのタイル鍵を生成し、暗号復号部に送信しなければならなかった。一方で、本実施形態においては、アクセス鍵生成処理部においてタイルインデックス2に対応する1つのタイル鍵だけを生成し、暗号復号部に送信するようにすればよく、効率的である。

#### 【0131】

また、各々のタイルパートに対する鍵は親のノードに対応するタイル鍵と、当該タイルパートのタイルパートインデックスとから、ハッシュ関数を用いて算出できる。例えば、第1の実施形態では、タイルパート1に対応するタイルパートだけへのアクセスを許可することは困難であった。これは、タイルパート1へアクセスを許可することは、同時にその子ノードに対応するタイルパート0への許可をアクセスすることになったからである。一方で、本実施形態においては、タイルパート1に対応するタイルパート鍵は、その親ノードに対応するタイル鍵と、当該タイルパートインデックス1から生成できるため、より柔軟なアクセス制御を実現可能である。

#### 【0132】

更に、図6におけるS63において、タイル鍵を(式2')のように生成し、

S 6 9において、タイルパート鍵を（式 3）のように生成したり、或いは、S 6 3において、タイル鍵を（式 2）のように生成し、S 6 9において、タイルパート鍵を（式 3'）のように生成するようにすることも可能であることは明らかである。

### 【0 1 3 3】

#### [第 4 の実施形態]

第 3 の実施形態においては、タイルパート鍵が、親ノードに対応するタイル鍵と、当該タイルパートに対応するタイルパートインデックスとから生成される例を説明した。更に、本実施の形態においては、タイルパート鍵がグループ化されて生成される例を説明する。

### 【0 1 3 4】

本実施形態におけるタイルパート鍵生成処理を図 1 7 を用いて説明する。図 1 7 は本実施形態におけるタイルパート鍵生成処理を説明するフローチャートである。図 6 に示したフローチャートにおける S 6 8 から S 7 4 までの処理を、図 1 7 に示す処理に置き換えるようにすればよい。

### 【0 1 3 5】

まず、ステップ S 1 7 1 において、パラメータ  $i$  及び  $j$  が“0”に初期化される。パラメータ  $i$  はツリー構造におけるレベルを示すインデックスであり、パラメータ  $j$  は各レベルにおけるノードを表すインデックスである。特に、 $i$  と  $j$  のくみあわせ ( $i, j$ ) をタイルパートグループインデックスと呼ぶ。

### 【0 1 3 6】

次のステップ S 1 7 2 では、タイルパートグループインデックス ( $i, j$ ) のタイルパートグループ鍵が生成される。タイルパートグループ鍵は、その親のタイルパートグループ鍵、及びタイルパートグループインデックス ( $i, j$ ) のハッシュ値として式 (4) のように算出される。

$$K(i, j) = H(K(i-1, k), i, j) \quad (\text{式 4})$$

ここで、 $k$  はタイルパートグループ ( $i, j$ ) の親ノードに対応するノードを表すインデックスである。即ち、親ノードに対応するタイルパートグループ鍵  $K(i-1, k)$  と、生成するタイルパートグループ鍵に対応するノードのタイル

パートグループインデックス ( $i, j$ ) とからタイルパートグループ鍵が生成される。しかしながら、本発明はこれに限定されることなく、親ノードに対応する鍵と、生成するタイルパートグループ鍵に対応するノードに含まれるタイルパートインデックスとからタイルパートグループ鍵を生成するようにしてもよい。

#### 【0137】

例えば、生成するタイルパートグループに対応するノードから順に木をたどり、タイルパートに対応するノードを調べ、当該タイルパートのタイルパートインデックスを用いるようにすれば良い。要するに、上位ノード（ルートノード側にあるノード）に対する鍵  $ck$  と、その下位（下層）方向にあるノードのインデックスに基づいて、下位にあるノードの鍵を派生することを順に繰り返すことになる。

#### 【0138】

ここで、（式4）を用いて生成されたタイルパートグループ鍵のうち、最も子ノードに位置するレベルの鍵はタイルパート鍵である。タイルパート鍵の場合には、生成した鍵を鍵行列  $ka$  に記録される。

#### 【0139】

ステップ S173 では、レベル  $i$  において全てのノードに対応するタイルパートグループ鍵が生成されたか否かが判定される。判定結果が真の場合はステップ S175 に進み、判定結果が偽の場合はステップ S174 に進む。

#### 【0140】

ステップ S174 では、パラメータ  $j$  が 1 だけ増やされ、その後ステップ S172 が再度処理される。つまり、パラメータ  $i$  で示されるレベルに属する全タイルパートグループについて鍵が生成されることになる。

#### 【0141】

一方、パラメータ  $i$  で示されるレベルに対するタイルパートグループ鍵が生成されると、処理はステップ S175 に進み、全てのレベルが処理されたか否かが判定される。判定結果が真の場合は処理を終了する。判定結果が偽の場合はステップ S176 に進んで、次のレベルの処理を行うべく、パラメータ  $i$  を 1 だけ増加させ、ステップ S172 以降の処理を繰り返す。

## 【0142】

以上のように、タイル部分をグループ化して鍵行列を生成することによって、複数のタイル部分に対するアクセス制御をする際にはタイル部分グループ鍵をアクセス鍵生成処理部で生成するようにすればよく、効率的にアクセス制御することが可能となる。

## 【0143】

また以上説明した実施形態における、暗号化処理部141、アクセス鍵生成処理部142、更には、復号処理部143は、それぞれパーソナルコンピュータ等の情報処理装置でもって実現できるし、その機能を実現する手順としての方法の発明として捉えることができる。また、コンピュータにより実現できるわけであるから、本発明はそれぞれの装置で実行されるコンピュータプログラム、更には、そのコンピュータプログラムを格納し、コンピュータが読み込めるCDROM等のコンピュータ可読記憶媒体にも適用できるのは明らかであろう。

## 【0144】

従って、上記実施形態に係る実施態様を列举すると、次の通りである。すなわち、暗号化処理部141としての情報処理方法及び装置、並びにコンピュータプログラム及びコンピュータ可読記憶媒体は、次のようになる。

## 【0145】

〔実施態様1〕 タイル単位に圧縮符号化された符号化画像データを入力し、暗号化する情報処理方法であって、

隣接する複数のタイルで1つのタイルグループを構成し、更に、隣接する複数のタイルグループで1つの更なるタイルグループを構成することを繰り返すことでタイル及びタイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義し、

前記符号化画像データで表現される画像全体から、前記ツリー構造の最上位層にあるノードに対する暗号化鍵情報を生成し、

注目ノードの暗号化鍵情報を、上位のノードに対して生成された暗号化鍵情報

に基づいて生成することを、末端に位置するノードまで繰り返し行ない、

前記ツリー構造における、前記部分符号化データのノード中の所望とするノード位置を暗号化対象とする指定入力を与えられた場合、当該指定入力されたノード位置の部分符号化データを含み、高位に位置する部分符号化データを暗号化対象として設定し、

暗号化を行うよう設定された個々の部分符号化データに対し、当該部分符号化データに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した部分符号化データ及び暗号化されていない部分符号化データを出力する

ことを特徴とする情報処理方法。

#### 【0146】

〔実施態様2〕 前記暗号化鍵情報は、上位階層から下位階層に向かう一方向性を有する関数を用いて生成することを特徴とする実施態様1に記載の情報処理方法。

#### 【0147】

〔実施態様3〕 前記関数は、下位階層にあるタイルグループ、タイル、部分符号化データの座標位置情報をパラメータとして鍵情報を生成することを特徴とする実施態様2に記載の情報処理方法。

#### 【0148】

〔実施態様4〕 前記最上位階層の暗号化鍵情報は、所定のインターネット上の認証用サーバに出力することを特徴とする実施態様1に記載の情報処理方法。

#### 【0149】

〔実施態様5〕 更に、入力した符号化データを、タイル、タイルグループ、部分符号化データの階層構造として表示する工程を備え、

前記所望とする階層の所望とする部分符号化データは、前記表示工程での表示された階層構造から指定することを特徴とする実施態様1に記載の情報処理方法。

#### 【0150】

〔実施態様6〕 タイル単位に圧縮符号化された符号化画像データを入力し、暗号化する情報処理装置であって、

隣接する複数のタイルで1つのタイルグループを構成し、更に、隣接する複数のタイルグループで1つの更なるタイルグループを構成することを繰り返すことでタイル及びタイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義する手段と、

前記符号化画像データで表現される画像全体から、前記ツリー構造の最上位層にあるノードに対する暗号化鍵情報を生成する手段と、

注目ノードの暗号化鍵情報を、上位のノードに対して生成された暗号化鍵情報に基づいて生成することを、末端に位置するノードまで繰り返し行なう手段と、

前記ツリー構造における、前記部分符号化データのノード中の所望とするノード位置を暗号化対象とする指定入力を与えられた場合、当該指定入力されたノード位置の部分符号化データを含み、高位に位置する部分符号化データを暗号化対象として設定する手段と、

暗号化を行うよう設定された個々の部分符号化データに対し、当該部分符号化データに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した部分符号化データ及び暗号化されていない部分符号化データを出力する手段と

を備えることを特徴とする情報処理装置。

#### 【0151】

〔実施態様7〕 コンピュータが読み込み実行することで、タイル単位に圧縮符号化された符号化画像データを入力し、暗号化する情報処理装置として機能するコンピュータプログラムであって、

隣接する複数のタイルで1つのタイルグループを構成し、更に、隣接する複数のタイルグループで1つの更なるタイルグループを構成することを繰り返すことでタイル及びタイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義する手段と、

前記符号化画像データで表現される画像全体から、前記ツリー構造の最上位層にあるノードに対する暗号化鍵情報を生成する手段と、

注目ノードの暗号化鍵情報を、上位のノードに対して生成された暗号化鍵情報に基づいて生成することを、末端に位置するノードまで繰り返し行なう手段と、

前記ツリー構造における、前記部分符号化データのノード中の所望とするノード位置を暗号化対象とする指定入力を与えられた場合、当該指定入力されたノード位置の部分符号化データを含み、高位に位置する部分符号化データを暗号化対象として設定する手段と、

暗号化を行うよう設定された個々の部分符号化データに対し、当該部分符号化データに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した部分符号化データ及び暗号化されていない部分符号化データを出力する手段と

して機能することを特徴とするコンピュータプログラム。

#### 【0152】

【実施態様8】 実施態様7に記載のコンピュータプログラムを格納すること  
を特徴とするコンピュータ可読記憶媒体。

#### 【0153】

また、復号処理部143としての情報処理方法及び装置、並びにコンピュータ  
プログラム及びコンピュータ可読記憶媒体は、次のようになる。

#### 【0154】

【実施態様9】 暗号化／非暗号化されたタイル単位の符号化データが混在し  
た情報を入力し、画像を再現する情報処理方法であって、

入力した情報に基づき、隣接する複数のタイルで1つのタイルグループを構成  
し、更に、隣接するタイルグループで1つの更なるタイルグループを構成するこ  
とを繰り返すことで、タイルグループの階層構造を定義し、当該階層構造の末端  
に位置するタイルの符号化データを構成する複数の部分符号化データについては  
、復号する際に優先するものほど末端に位置させることで、各タイルグループ、  
各タイル、各部分符号化データをノードするツリー構造を定義し、

暗号化された部分符号化データを包含するタイルに対する、暗号解除を行うた

めの鍵情報を入力し、

入力したタイルの鍵情報に基づき、注目タイルの下位に位置する所望とする部分符号化データまでの情報を順次生成し、

生成された各部分符号化データに対する鍵情報を用いて、暗号化された各部分符号化データの暗号化を解除し、復号する

ことを特徴とする情報処理方法。

#### 【0 1 5 5】

〔実施態様 1 0〕 暗号化／非暗号化されたタイル単位の符号化データが混在した情報を入力し、画像を再現する情報処理装置であって、

入力した情報に基づき、隣接する複数のタイルで 1 つのタイルグループを構成し、更に、隣接するタイルグループで 1 つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義する手段と、

暗号化された部分符号化データを包含するタイルに対する、暗号解除を行うための鍵情報を入力する手段と、

入力したタイルの鍵情報に基づき、注目タイルの下位に位置する所望とする部分符号化データまでの情報を順次生成する手段と、

生成された各部分符号化データに対する鍵情報を用いて、暗号化された各部分符号化データの暗号化を解除し、復号する手段と

を備えることを特徴とする情報処理装置。

#### 【0 1 5 6】

〔実施態様 1 1〕 コンピュータが読み込み実行することで、暗号化／非暗号化されたタイル単位の符号化データが混在した情報を入力し、画像を再現する情報処理装置として機能するコンピュータプログラムであって、

入力した情報に基づき、隣接する複数のタイルで 1 つのタイルグループを構成し、更に、隣接するタイルグループで 1 つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義し、当該階層構造の末端



に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義する手段と、

暗号化された部分符号化データを包含するタイルに対する、暗号解除を行うための鍵情報を入力する手段と、

入力したタイルの鍵情報に基づき、注目タイルの下位に位置する所望とする部分符号化データまでの情報を順次生成する手段と、

生成された各部分符号化データに対する鍵情報を用いて、暗号化された各部分符号化データの暗号化を解除し、復号する手段

として機能することを特徴とするコンピュータプログラム。

#### 【0157】

〔実施態様12〕 実施態様11に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

#### 【0158】

更に、アクセス鍵生成処理部142としてのサーバ及びその制御方法、並びにコンピュータプログラム及びコンピュータ可読記憶媒体は、次のようになる。

#### 【0159】

〔実施態様13〕 暗号化／非暗号化されたタイル単位の符号化データが混在した画像のための暗号解除鍵を提供するネットワークに接続されるサーバの処理方法であって、

1つのタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させ、隣接する複数のタイルで1つのタイルグループを構成し、更に、隣接するタイルグループで1つの更なるタイルグループを構成することを繰り返す階層構造を有する画像の最上位に位置する基本解除鍵情報を記憶し、

解除させたい部分符号化データを指定する情報を前記ネットワーク上のクライアントから受信したとき、指定された階層の指定された部分符号化データに到達するまで、前記基本解除鍵から下位層に向かって順次解除鍵情報を派生し、該当する部分符号化データに対する解除鍵情報が生成された場合に、当該解除鍵情報

を前記クライアントに通知する

ことを特徴とするサーバの処理方法。

【0 1 6 0】

〔実施態様 1 4〕 暗号化／非暗号化されたタイル単位の符号化データが混在した画像のための暗号解除鍵を提供するネットワークに接続されるサーバであって、

1 つのタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させ、隣接する複数のタイルで 1 つのタイルグループを構成し、更に、隣接するタイルグループで 1 つの更なるタイルグループを構成することを繰り返す階層構造を有する画像の最上位に位置する基本解除鍵情報を記憶する手段と、

解除させたい部分符号化データを指定する情報を前記ネットワーク上のクライアントから受信したとき、指定された階層の指定された部分符号化データに到達するまで、前記基本解除鍵から下位層に向かって順次解除鍵情報を派生し、該当する部分符号化データに対する解除鍵情報が生成された場合に、当該解除鍵情報を前記クライアントに通知する手段と

を備えることを特徴とするサーバ。

【0 1 6 1】

〔実施態様 1 5〕 コンピュータが読み込み実行することで、暗号化／非暗号化されたタイル単位の符号化データが混在した画像のための暗号解除鍵を提供するネットワークに接続されるサーバとして機能するコンピュータプログラムであって、

1 つのタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させ、隣接する複数のタイルで 1 つのタイルグループを構成し、更に、隣接するタイルグループで 1 つの更なるタイルグループを構成することを繰り返す階層構造を有する画像の最上位に位置する基本解除鍵情報を記憶する手段と、

解除させたい部分符号化データを指定する情報を前記ネットワーク上のクライアントから受信したとき、指定された階層の指定された部分符号化データに到達

するまで、前記基本解除鍵から下位層に向かって順次解除鍵情報を派生し、該当する部分符号化データに対する解除鍵情報が生成された場合に、当該解除鍵情報を前記クライアントに通知する手段

として機能することを特徴とするコンピュータプログラム。

#### 【0162】

〔実施態様16〕 実施態様15に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

#### 【0163】

##### 【発明の効果】

以上説明したように本発明によれば、個々のタイルが複数の部分符号化データで構成され、その部分符号化データが階層構造を有する画像データに対して、各部分符号化データ毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がないようにすることが可能となる。

##### 【図面の簡単な説明】

##### 【図1】

本実施形態における暗号処理部のブロック構成図である。

##### 【図2】

本実施形態におけるタイル及びタイルパートを示す図である。

##### 【図3】

本実施形態におけるタイルグループ化を説明するための図である。

##### 【図4A】

第1の実施形態におけるタイルパート、及びタイルグループのツリー構造を示す図である。

##### 【図4B】

図4Aのツリー構造をタイルインデックス、タイルパートインデックスで示すツリー構造図である。

##### 【図5】

本実施形態における暗号化対象タイルパート情報を説明する図である。

##### 【図6】

本実施形態における鍵行列生成処理のフローチャートである。

【図 7】

本実施形態における鍵行列の構造を示す図である。

【図 8】

本実施形態における暗号化タイルパート行列の一例を示す図である。

【図 9】

本実施形態におけるアクセス鍵生成処理部のブロック構成図である。

【図 1 0】

本実施形態におけるアクセス鍵のフォーマットを示す図である。

【図 1 1】

本実施形態における復号処理部のブロック構成図である。

【図 1 2】

本実施形態における鍵行列生成処理を説明する図である。

【図 1 3】

本実施形態における暗号化タイルパート情報の一例を示す図である。

【図 1 4】

本実施形態におけるシステムの全体構成図である。

【図 1 5】

タイルパートの他の形態を示す図である。

【図 1 6】

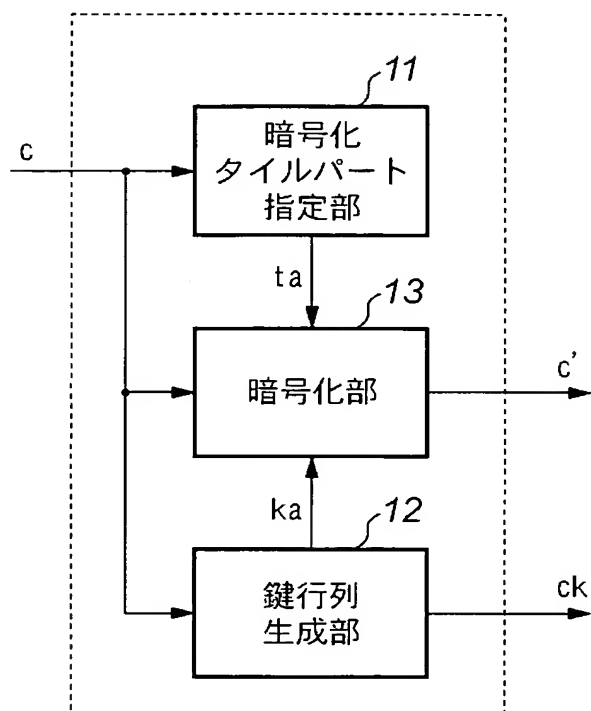
第 3 の実施形態におけるタイルパート、及びタイルグループのツリー構造を示す図である。

【図 1 7】

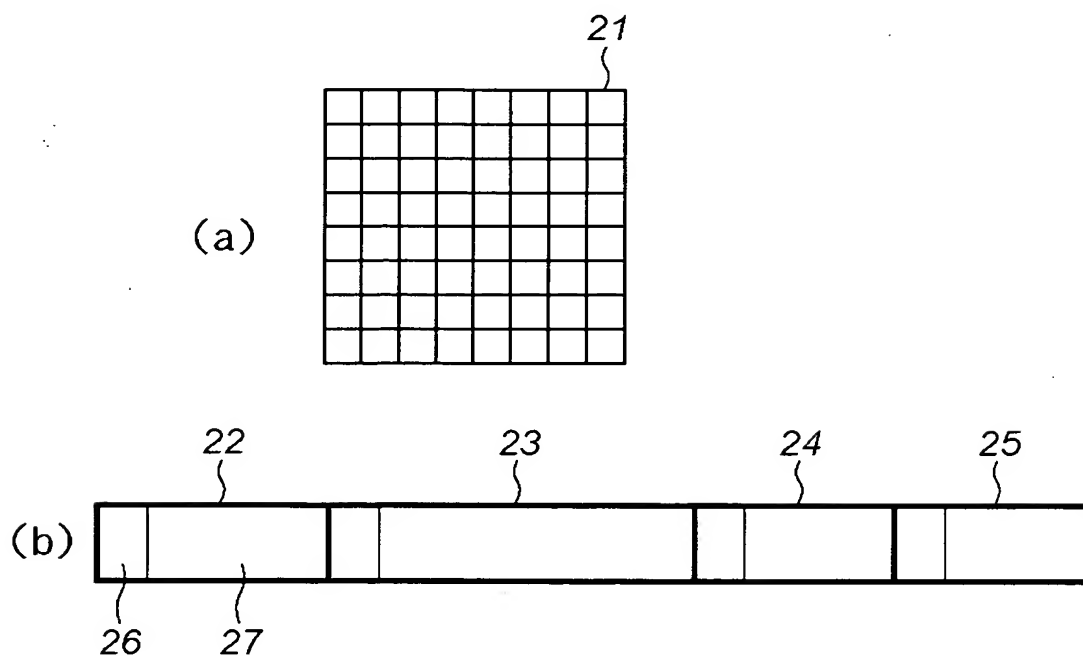
第 4 の実施形態における処理の一部分を示すフローチャートである。

【書類名】 図面

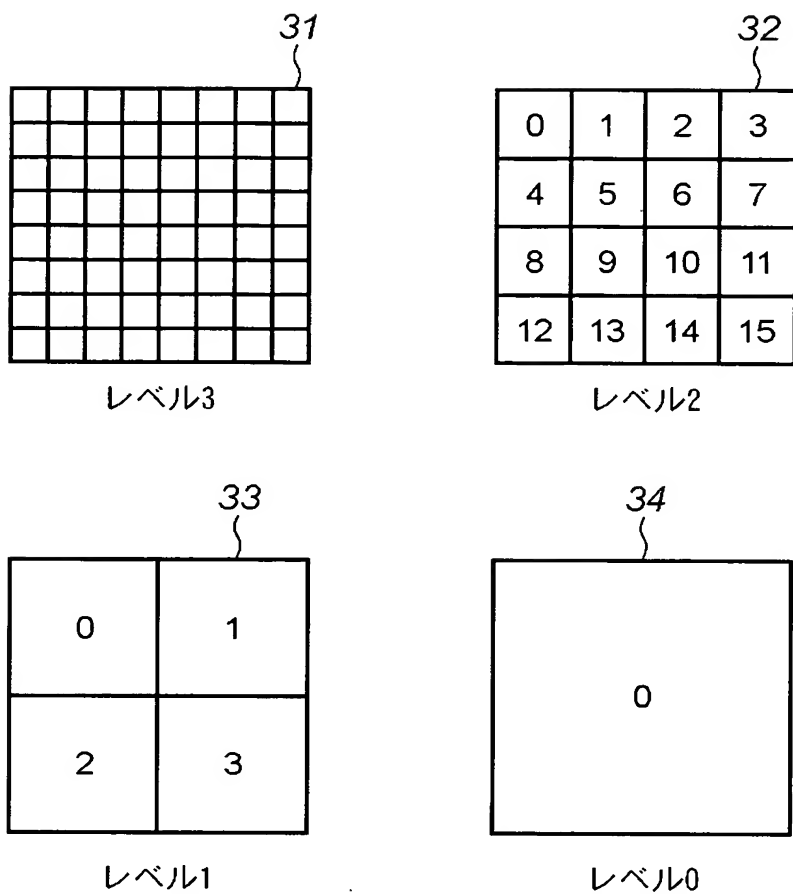
【図 1】



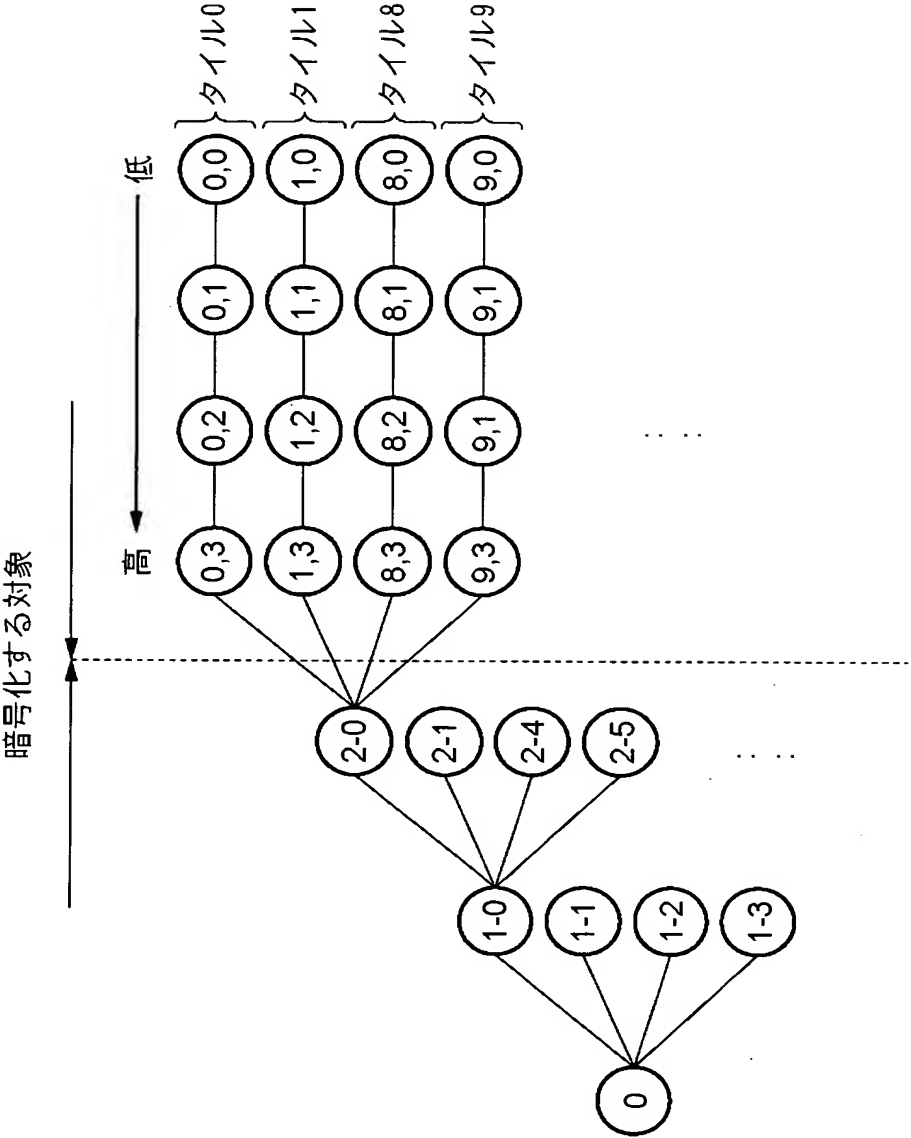
【図 2】



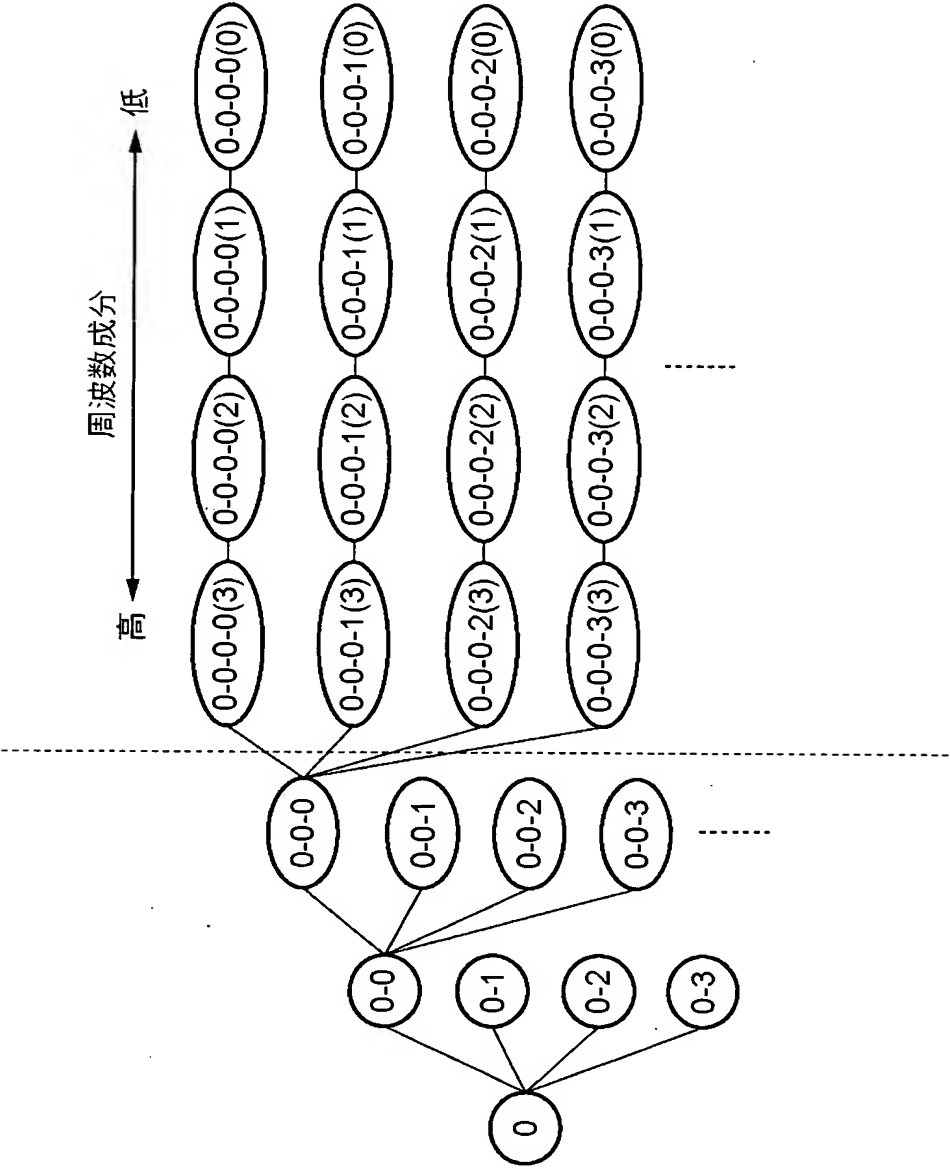
【図 3】



【図 4 A】



【図 4 B】

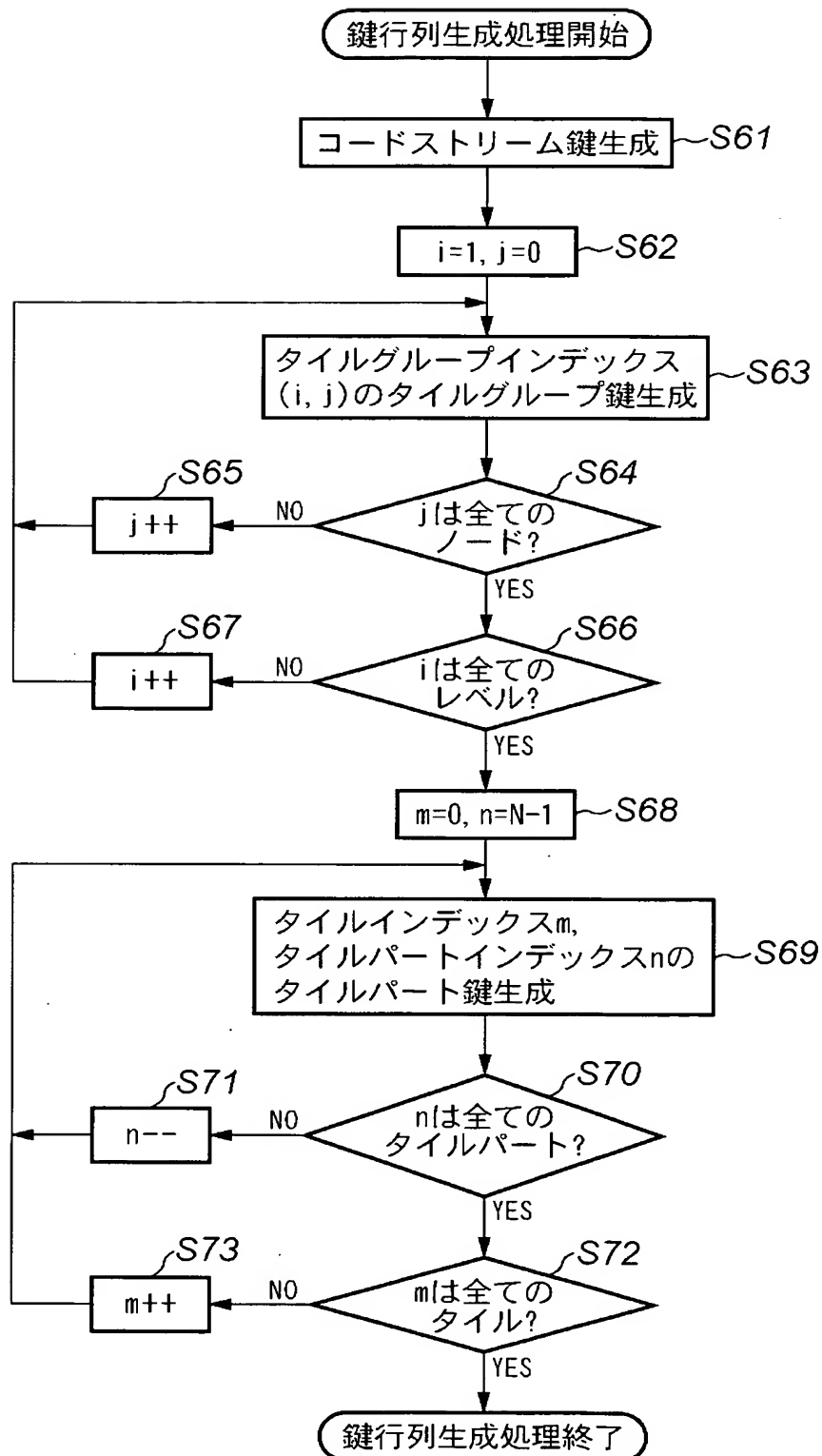




【図 5】

タイルインデックス	暗号化されるタイルパート インデックスの最小値
0	0
1	2
3	3
4	1
5	0
:	:
62	3
63	1

【図 6】



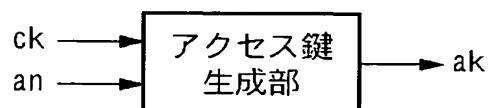
【図 7】

	0	1	2	3	4	5
0						
1						
3						
4						
5						
:						
62						
63						

【図 8】

	0	1	2	3	4	5
0	1	1	1	1	1	1
1	0	1	1	1	2	2
3	0	0	0	1	1	2
4	0	1	1	1	1	2
5	1	1	1	1	2	2
:	:	:	:	:	:	:
62	0	0	0	1	1	2
63	0	1	1	1	2	2

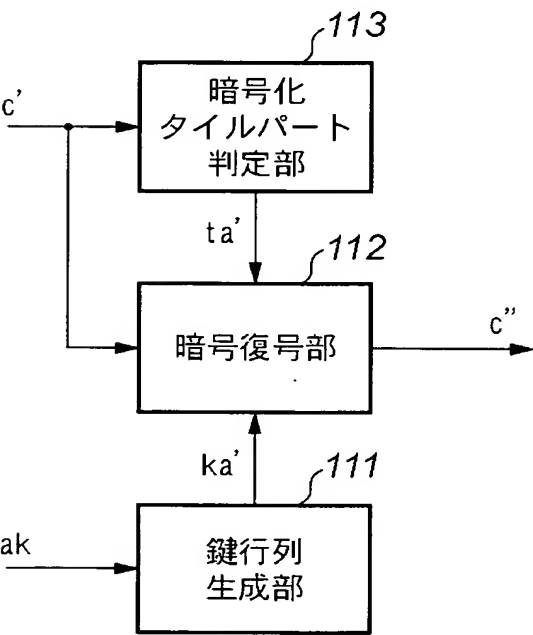
【図 9】



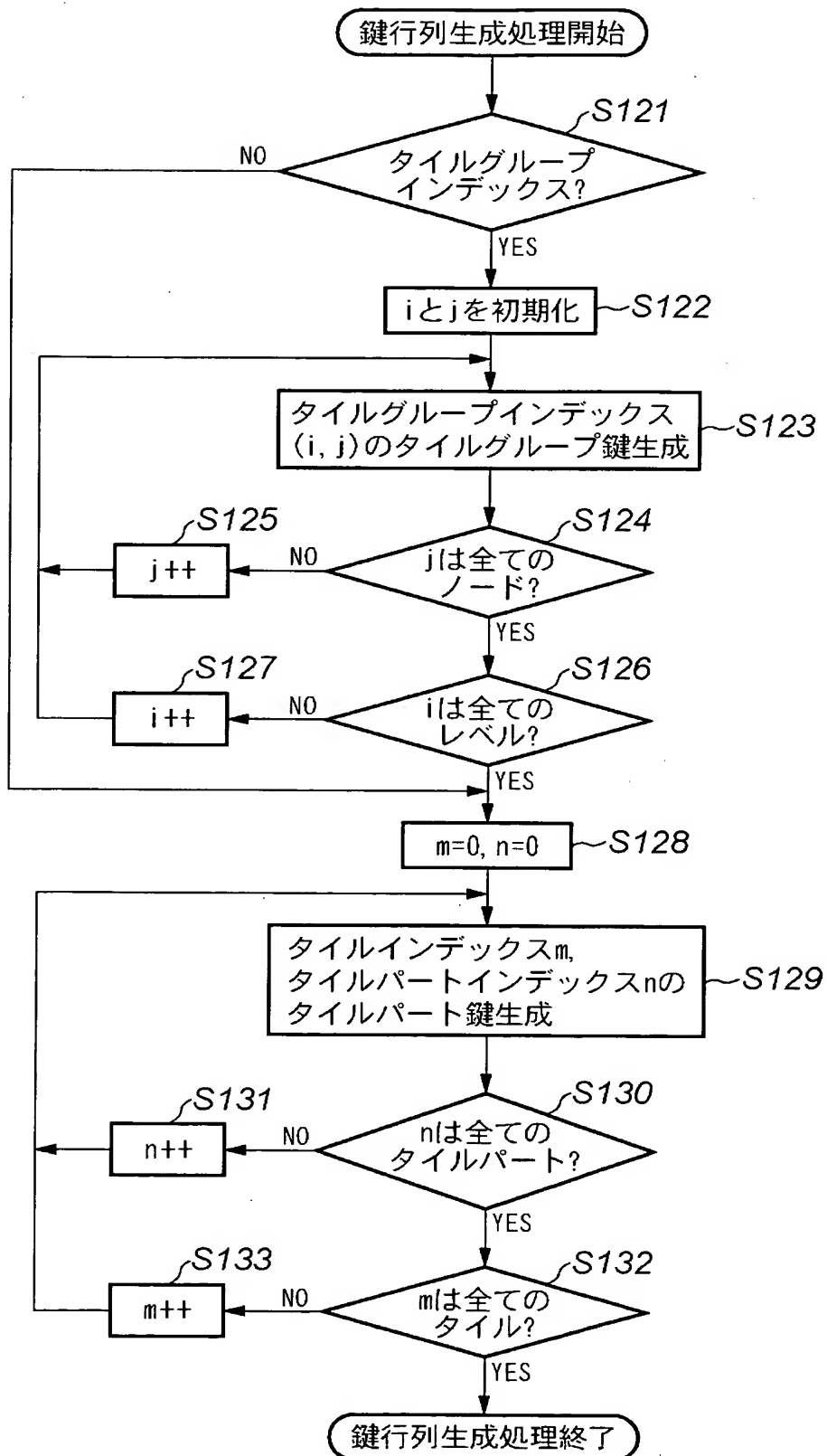
【図 1 0】

アクセス鍵値
アクセス鍵値に対応するインデックス
タイルパートインデックスかタイル グループインデックスかを示す情報

【図 1 1】



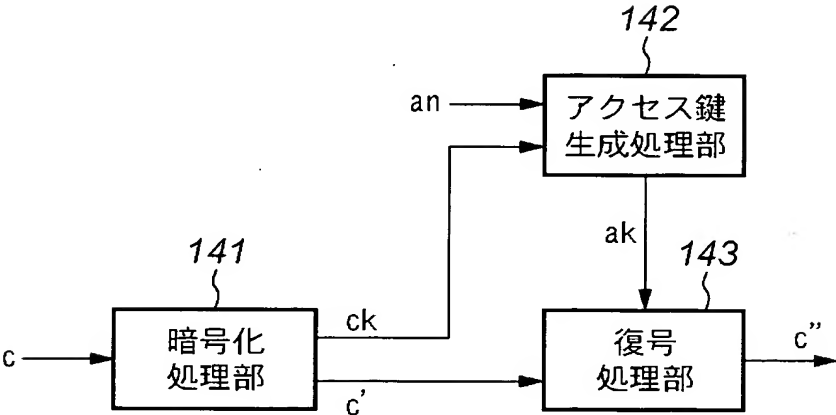
【図 12】



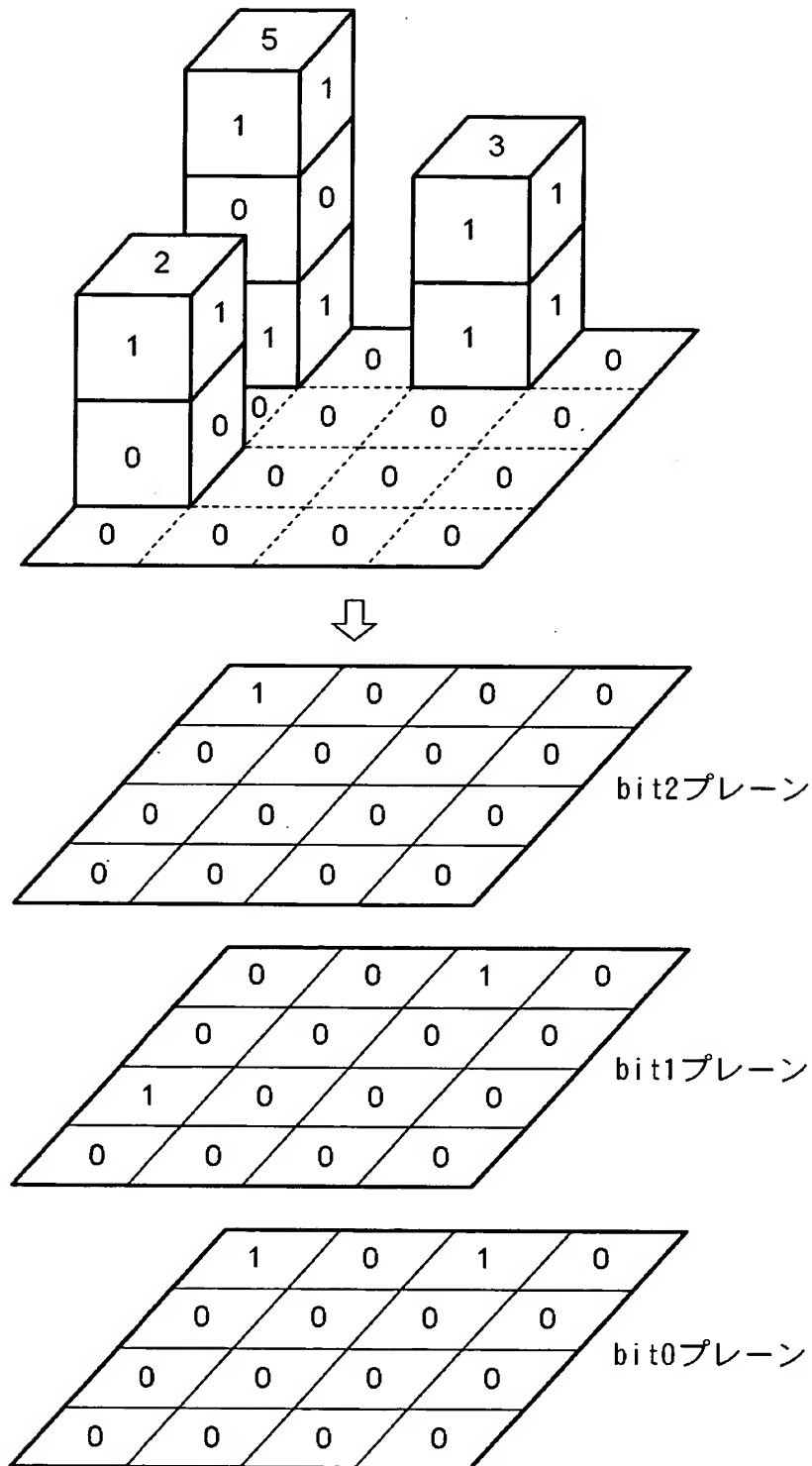
【図 1 3】

	0	1	2	3	4	5
0	1	1	1	1	1	1
1	0	0	1	1	2	2
2	0	0	0	1	1	2
3	0	1	1	1	1	2
4	1	1	1	1	2	2
⋮	⋮	⋮	⋮	⋮	⋮	⋮
62	0	0	0	1	1	2
63	0	1	1	1	2	2

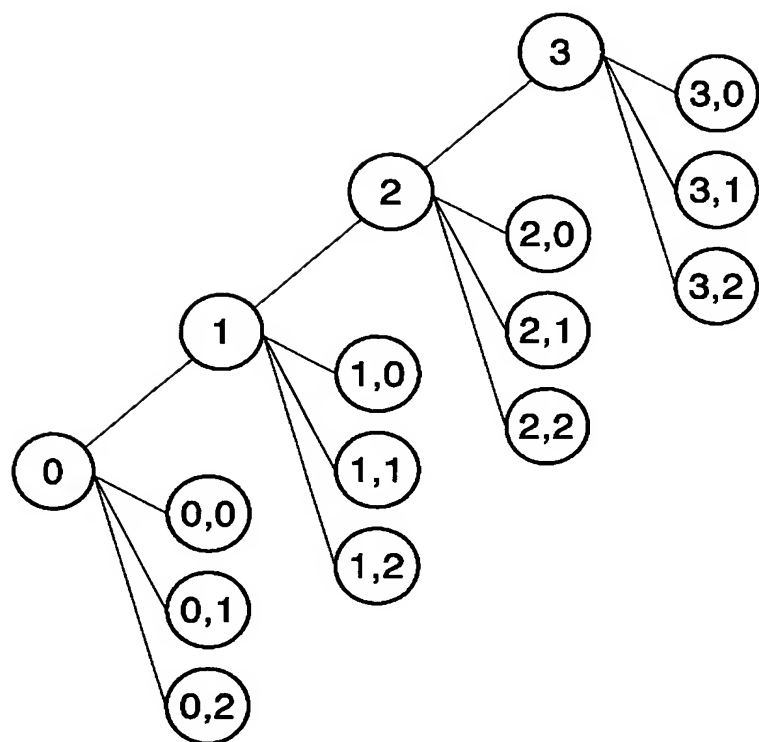
【図 1 4】



【図 15】

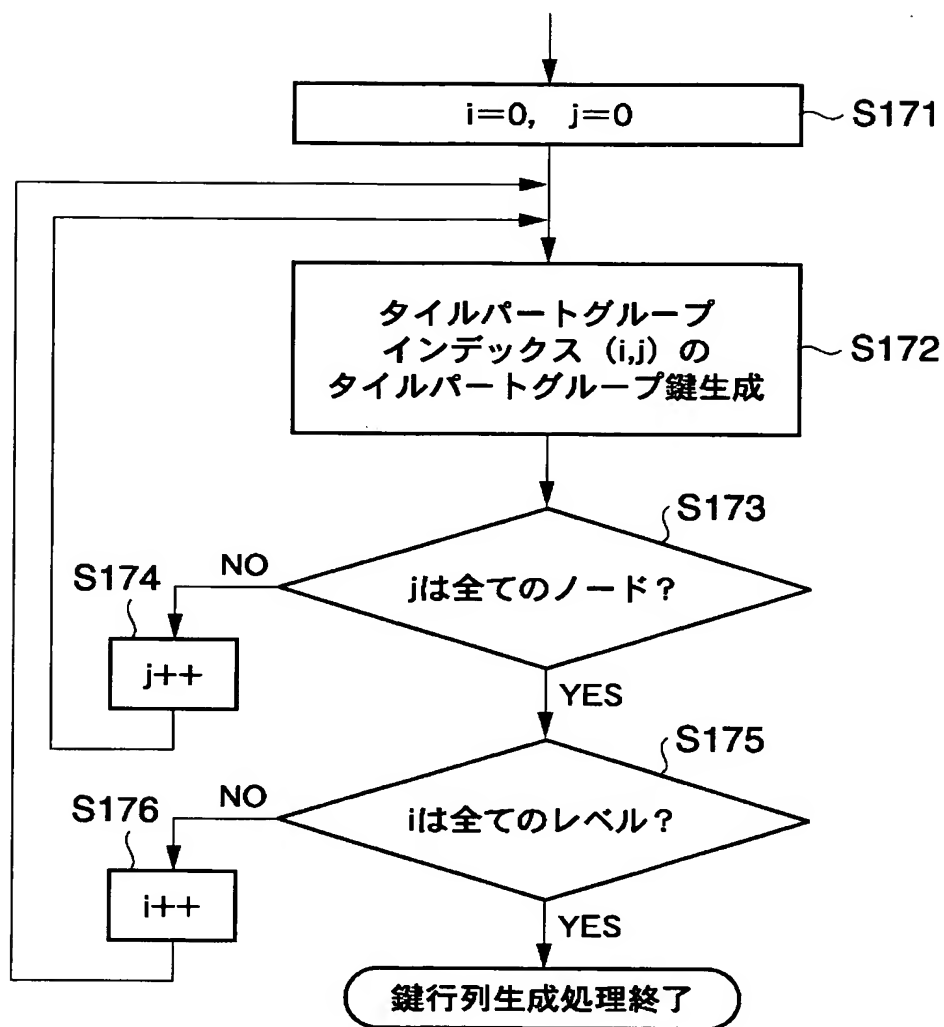


【図 16】





【図 17】



**【書類名】 要約書****【要約】**

**【課題】** 画像の符号化する単位のタイルが複数の部分符号化データで構成され、その部分符号化データが階層構造を有する画像データに対して、各部分符号化データ毎に異なる暗号鍵を用いた場合にも、複数の鍵の管理を不要にする。

**【解決手段】** 圧縮符号化単位であるタイルが複数の部分符号化データで構成されるコードストリーム  $c$  を入力する。暗号化タイルパート指定部は、隣接する複数のタイルで 1 つのタイルグループを構成し、更に、隣接するタイルグループで 1 つの更なるタイルグループを構成することを繰り返してタイル及びタイルグループの階層構造を定義し、当該階層構造の末端に位置するタイルの符号化データを構成する複数の部分符号化データについては、復号する際に優先するものほど末端に位置させることで、各タイルグループ、各タイル、各部分符号化データをノードするツリー構造を定義したとき、どの階層のどのタイルの部分符号化データまで暗号化を行うかを決定し、暗号化タイル情報  $t_a$  として出力する。一方、鍵行列生成部 12 は、入力したコードストリーム  $c$  の全体に対する暗号化鍵  $c_k$  を生成し、階層構造の各ノードの暗号化鍵を次々に生成し、その結果を鍵行列  $k_a$  として出力する。暗号化部 13 は、暗号化対象となるタイルの部分符号化データ用に生成された鍵を用いて暗号化し、コードストリーム  $c'$  を出力する。

**【選択図】 図 1**

特願 2 0 0 2 - 3 0 4 4 9 7

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 1 0 0 7 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キャノン株式会社